UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,403	06/19/2001	Sundeep M. Bajikar	219.40074X00	1335

23838 7590 01/13/2005

KENYON & KENYON
1500 K STREET, N.W., SUITE 700
WASHINGTON, DC 20005

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/883,403	BAJIKAR, SUNDEEP M.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6/19/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claims 1-30 contain the trademark Bluetooth. Where a trademark is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark cannot be used properly to identify any particular material or product. A trademark is used to identify a source of goods, and not the goods themselves. Thus, a trademark does not identify or describe the goods associated with the trademark. In the present case, the trademark is used to identify/describe a protocol for wireless device communication and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4,7,18-21,24, and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Cromer et al.

The examiner notes that since the trademark "Bluetooth" is claimed, the examiner is interpreting the usage of "Bluetooth" as being wireless communications.

As per claims 1,18, and 29, Cromer et al discloses of a system, method and computer readable medium having stored thereon a plurality of instructions that are executed by a processor for a wireless communication system (col. 1, lines 36-37 & col. 2, lines 23-26). A computer (secured device) is equipped with wireless technology (col. 1, lines 37-40 & col. 4, lines 28-33). A plurality of RFID interfaces (access points) are located at designated points to establish a wireless link with the computer (secured device)(col. 1, lines 37-40 & col. 4, lines 28-33). A shipping site (security server) is connected to the RFID interfaces (access points) and arranged to provide access control and security services for the computer (secured device)(col. 3, line 66 through col. 4, line 4). The security server obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4). The teachings of Cromer et al disclose of storing this information in a central database and marks the device as shipped (col. 4, lines 10-22), so it is

interpreted by the examiner that this is the last known location of the computer (secured device). A lock code is activated with the computer (secured device), via the RFID interface (access point), to disable it from being operational and it is then re-enabled via the RFID interface (access point) upon arrival to its destination (location)(col. 1, lines 37-45 & col. 5, lines 14-22).

As per claims 2 and 19, Cromer et al teaches of attribute information of the computers (secured devices) is captured via the RFID interfaces (access points) and stored (registered) in a database at the shipping site (security server)(col. 3, line 66 through col. 4, line 12).

As per claims 3 and 20, it is disclosed by Cromer et al that the lock is activated between the computer (secured device) and the shipping site (security server) via the RFID interface (access point) upon a request from the computer (secured device)(col. 1, lines 37-45, col. 3, line 66 through col. 4, line 12, & col. 5, lines 14-22).

As per claims 4 and 21, Cromer et al discloses of a shipping site (security server) that is connected to the RFID interfaces (access points) and arranged to provide access control and security services for the computer (secured device)(col. 3, line 66 through col. 4, line 4). The security server obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4). The teachings of Cromer et al disclose of storing this information in a central database and marks the device as shipped (col. 4, lines 10-22), so it is interpreted by the examiner that this is the last known location of the computer (secured device).

As per claims 7 and 24, it is disclosed by Cromer et al that a computer (secured device) sends back to the shipping site (security server) an unlock code to disengage the lock thereby making the computer (secured device) free to roam (col. 1, lines 36-46 & col. 4, lines 33-52).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5,6,8,9,22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al in view of Elledge.

As per claims 5 and 22, the teachings of Cromer et al disclose of disabling a computer (secured device) via an RFID interface (access point). A shipping site (security server) obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4) and storing this information in a central database and marks the device as shipped (col. 4, lines 10-22). The teachings of Cromer et al are silent in disclosing of remote tracking and monitoring of the secured device. It is disclosed by Elledge of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply usage of monitoring and tracking devices.

Elledge discloses of motivational benefits by teaching that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). It is obvious that the teachings of Cromer et al would have further benefited from the disclosure of Elledge as a means of further locating lost or stolen devices by monitoring and tracking.

As per claims 6 and 23, the teachings of Cromer et al disclose of disabling a computer (secured device) via an RFID interface (access point). A shipping site (security server) obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4) and storing this information in a central database and marks the device as shipped (col. 4, lines 10-22). If an incorrect password is signaled to the compute (secured device), it remains disabled (remaining in an unauthorized disconnection)(col. 4, lines 52-60). The teachings of Cromer et al are silent in disclosing of notifying the owner of the computer (secured device). Elledge discloses of remotely monitoring and tracking of secured devices through usage of RFID interfaces and the proper authorities (owner) can be notified (col. 2, lines 20-24,27-43, & 38-43). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply usage of monitoring and tracking devices. Elledge discloses of motivational benefits by teaching that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and

tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). It is obvious that the teachings of Cromer et al would have further benefited from the disclosure of Elledge as a means of further locating lost or stolen devices by monitoring and tracking.

As per claims 8 and 25, the teachings of Cromer et al disclose that a shipping site (security server) is connected to the RFID interfaces (access points) and arranged to provide access control and security services for the computer (secured device)(col. 3, line 66 through col. 4, line 4). The security server obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4). The teachings of Cromer et al disclose of storing this information in a central database and marks the device as shipped (col. 4, lines 10-22), so it is interpreted by the examiner that this is the last known location of the computer (secured device). The teachings involve usage of a CPU (processor) and I/O subsystem and security software dictates changes, settings, and configuration of the computer (secured device)(col. 1, lines 37-40 & col. 2, lines 42-58). The connections are established across the Internet (col. 4, lines 25-27). The teachings of Cromer et al are silent in disclosing of remote tracking and monitoring of the secured device. It is disclosed by Elledge of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply usage of monitoring and tracking devices. Elledge discloses of motivational benefits by teaching that devices are either lost or stolen and owners have no way of locating and

retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). It is obvious that the teachings of Cromer et al would have further benefited from the disclosure of Elledge as a means of further locating lost or stolen devices by monitoring and tracking.

As per claim 9, it is taught by Cromer et al of a CPU (processor), a host chipset connected to the CPU (processor), a memory connected to the host chipset and arranged to contain an operating system and security control software for activating/deactivating a lock with the RFID interfaces (access points)(col. 1, lines 37-45, col. 2, lines 42-58, & col. 5, lines 14-22). An RFID interface (transceiver) connected to the host chip set and arranged to contain an antenna complex for establishing communication with any RFID interfaces (access points) for security services (col. 2, lines 35-58 & col. 3, lines 44-56).

8. Claims 10-17 and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al in view of Elledge in further view of Struble et al.

As per claim 10, the teachings of Cromer et al disclose of an RFID interface (transceiver) connected to the host chip set and arranged to contain an antenna complex for establishing (radio) communication with any RFID interfaces (access points) for security services (col. 2, lines 35-58 & col. 3, lines 44-56). The teachings of Elledge are relied upon of the usage of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43) wherein the benefit of

Elledge lies in the fact that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). The combination of the teachings of Cromer et al and Elledge fail to disclose of the use of Global Positioning System (GPS) receiver to determine a change in location. It is taught by Struble of a GPS system that helps recover a location of an article (secured device)(col. 11, lines 38-41). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply usage of a GPS system. The motivational benefits of using GPS help locate lost or stolen articles (secured devices) so that they can be recovered and returned to the proper owner (col. 11, lines 38-54).

As per claim 11, it is taught by Cromer et al of the RFID interfaces (wireless transceivers) having a unique device identification of the computer (secured device) for identification and communication with any of the access points strategically located at designated points where the computer (secured device) is secured temporarily (col. 3, line 66 through col. 4, line 13).

As per claim 12, it is disclosed by Cromer et al of a radio-frequency unit arranged to transmit/receive radio waves to/from any of the RFID interfaces (access points) via the antenna complex (col. 2, lines 35-41 & col. 3, lines 44-52). A baseband unit is arranged to establish link setup and support for link management between the computer (secured device) and the RFID interfaces (access points) which includes user authentication and authorization (col. 4, lines 4-42). The teachings of Cromer et al

disclose of a processor and storing the computer (secured device) information in a central database and marks the device as shipped (col. 2, lines 48-51 & col. 4, lines 10-22), so it is interpreted by the examiner that this is the last known location of the computer (secured device).

As per claim 13, the teachings of Cromer et al disclose of an RFID interface (transceiver) connected to the host chip set and arranged to contain an antenna complex for establishing (radio) communication with any RFID interfaces (access points) for security services (col. 2, lines 35-58 & col. 3, lines 44-56). The teachings of Elledge are relied upon of the usage of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43) wherein the benefit of Elledge lies in the fact that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). The teachings of Struble are relied upon for the disclosure of a GPS system that helps recover a location of an article (secured device)(col. 11, lines 38-41).

As per claims 14 and 25, the teachings of Cromer et al disclose of disabling a computer (secured device) via an RFID interface (access point). A shipping site (security server) obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4) and storing this information in a central database and marks the device as shipped (col. 4, lines 10-22). A lock code is activated with the computer (secured device), via the RFID

interface (access point), to disable it from being operational and it is then re-enabled via the RFID interface (access point) upon arrival to its destination (location)(col. 1, lines 37-45 & col. 5, lines 14-22). The teachings of Elledge are relied upon for disclosing of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43) wherein the benefit of Elledge lies in the fact that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). The combination of the teachings of Cromer et al and Elledge fail to disclose of using (X,Y,Z) coordinates of the last known location. It is taught by Struble of a GPS system, or (X,Y,Z) coordinates, that helps recover a location of an article (secured device)(col. 11, lines 38-41). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply usage of a GPS system, or (X,Y,Z) coordinates. The motivational benefits of using GPS help locate lost or stolen articles (secured devices) so that they can be recovered and returned to the proper owner (col. 11, lines 38-54).

As per claims 15 and 26, it is disclosed by Cromer et al that a security server obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4). The teachings of Cromer et al disclose of storing this information in a central database and marks the device as shipped (col. 4, lines 10-22). A lock code is activated with the computer (secured device), via the RFID interface (access point), to disable it from being

operational and it is then re-enabled via the RFID interface (access point) upon arrival to its destination (location)(col. 1, lines 37-45 & col. 5, lines 14-22). The teachings of Elledge are relied upon for disclosing of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43) wherein the benefit of Elledge lies in the fact that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval of the secured devices (col. 2, lines 20-24,38-43). The teachings of Struble are relied upon for the use of a GPS system, or (X,Y,Z) coordinates, that helps recover a location of an article (secured device)(col. 11, lines 38-41).

As per claims 16 and 27, it is disclosed by Cromer et al that a security server obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4). The teachings of Cromer et al disclose of storing this information in a central database and marks the device as shipped (col. 4, lines 10-22). A lock code is activated with the computer (secured device), via the RFID interface (access point), to disable it from being operational and it is then re-enabled via the RFID interface (access point) upon arrival to its destination (location)(col. 1, lines 37-45 & col. 5, lines 14-22). The teachings of Elledge are relied upon for disclosing of remotely monitoring and tracking of secured devices through usage of RFID interfaces (col. 2, lines 27-43) wherein the benefit of Elledge lies in the fact that devices are either lost or stolen and owners have no way of locating and retrieving the device once it is lost or stolen (col. 1, lines 16-21) and by

monitoring and tracking these devices, the appropriate personal can be notified to aid in retrieval (by a search and arrest request) of the secured devices (col. 2, lines 20-24,38-43). The teachings of Struble are relied upon for the use of a GPS system, or (X,Y,Z) coordinates, that helps recover a location of an article (secured device)(col. 11, lines 38-41).

As per claims 17 and 28, it is disclosed by Cromer et al that the lock is deactivated if the user at the computer (secured device) inputs the unlock code and the user supplied code matches the stored unlock code (col. 4, lines 48-59).

9. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al in view of Struble et al.

The teachings of Cromer et al disclose of disabling a computer (secured device) via an RFID interface (access point). A shipping site (security server) obtains attribute information of the computer (secured device) that includes a unique device identification number (col. 3, line 66 through col. 4, line 4) and storing this information in a central database and marks the device as shipped (col. 4, lines 10-22). A lock code is activated with the computer (secured device), via the RFID interface (access point), to disable it from being operational and it is then re-enabled via the RFID interface (access point) upon arrival to its destination (location)(col. 1, lines 37-45 & col. 5, lines 14-22). The teachings of Cromer et al fail to disclose of determination of the last known location of an article. It is taught by Struble of a GPS system that helps recover a location of an article (secured device)(col. 11, lines 38-41). It would have been obvious to a person of

ordinary skill in the art at the time of the invention to have been motivated to apply usage of a GPS system. The motivational benefits of using GPS help locate lost or stolen articles (secured devices) so that they can be recovered and returned to the proper owner (col. 11, lines 38-54).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Please see attached PTO-892

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/6/05
Christopher Revak
AU 2131

CR

January 6, 2005